An Anonymous Credit Card System

Elli Androulaki and Steven Bellovin
{elli,smb}@cs.columbia.edu

Columbia University

Abstract. Credit cards have many important benefits; however, these same benefits often carry with them many privacy concerns. In particular, the need for users to be able to monitor their own transactions, as well as bank's need to justify its payment requests from cardholders, entitle the latter to maintain a detailed log of all transactions its credit card customers were involved in. A bank can thus build a profile of each cardholder even without the latter's consent. In this paper, we present a practical and accountable anonymous credit system based on ecash , with a privacy preserving mechanism for error correction and expense-reporting.

1 Introduction

Motivation: Credit Cards vs. Consumer's Privacy. Credit cards have many useful properties. Apart permitting delayed payment, they provide users with logs of their own transactions, receipts, and the opportunity to challenge and correct erroneous charges. However, these same benefits are a privacy risk: banks can use the same information to build and sell profiles of their customers. We need a system that preserves the benefits of credit cards without violating users' privacy.

In the context of e-commerce, privacy of an entity is being able to transact with other entities without any unauthorized outsider being able to acquire any transaction-related information. In addition, no party should be able to build profiles of any other party based on purchases without the latter's consent. Being closely related to their owners'identities, credit cards' extended use constitutes a serious threat to consumers' privacy: *Frequent occurrences of credit card losses, credit card number based-impersonation attacks as well as human nature errors, i.e. overcharge of a client, make it necessary for cardholders to be able to monitor their own transaction activity and for merchants to provide banks with detailed description of each credit card transaction. Under the umbrella of the need of immediate charge justification/correction, each bank, which is no more*

In Proceedings of *6th International Conference on Trust, Privacy & Security in Digital Business. (TrustBus)*, 2009

trusted than the people operating it, acquires a global view of its customers' transaction activity. None of the currently deployed credit card systems offer consumer's privacy towards banks. Given the fact that the percentage of credit card-based purchases is increasing, a deployable privacy preserving credit card system has become quite important. This is the problem we have solved.

Privacy Preserving Payment Mechanisms. A very detailed report on the state of the art of electronic payment systems was first done by Asokan e.t.l. in [AJSW99]. [K99] and [BBG$^+$00] are credit card related protocols securing or blinding credit card information from third parties or merchant respectively but *not towards banks*. Credit Cards providing cardholder anonymity even towards the banks were introduced in 1994 by Low etl. [LPM94]. However, their scheme involves many trusted parties and offers no expense report or error correction service. Current schemes have some of the privacy problems mentioned earlier:
Ecash. Ecash [CHL05,DCN90] is a substitute of money on the Internet which cannot be faked, copied or spent more than once. It is known to provide absolute anonymity, namely no one can relate a particular ecash coin (ecoin) with its owner. One would argue that ecash could solve the problem we described before. Consumers can indeed buy anonymous ecoins from a bank/mint and use them in their online transactions. [B95] is a ecash based electronic payment system taking in consideration real world system threats. However, ecash is a prepayment based — as opposed to the most popular credit based — scheme, and used strictly for online transactions; additionally, the complete anonymity it guarantees gives no opportunities for error correction or expense reporting.
Anonymous Debit Cards(ADCs). Anonymous Debit Cards are prepaid ecash - based cards, which are recharged by cardholders and used to pay for goods anonymously. However, their use is very limited; among the reasons are the lack of error correction and proof of purchase mechanisms; additionally, they operate in a debit rather than a credit fashion, i.e. the amount of money paid by it, is subtracted from one's account, when the card is initially obtained.

Our Contribution. In this paper we introduce a privacy-preserving credit card mechanism which can be applied in current credit card systems. In particular, we present a realizable protocol to support "credit card"-based online and offline transactions, in which banks, unless authorized by the cardholder, do not acquire any knowledge of their customers' transactions. At the same time, cardholders are provided with detailed reports regarding their purchases and may participate on any type of merchant credit card offers. For the purposes of our system, we made use of a combination of two types of the compact ecash [CHL05] scheme for payments, and a combination of blind [CL02] and plain digital signatures

for the rest of our system's operations.

In the following sections we will briefly present our system's main functions. For space reasons, we have put the more detailed presentation of all the services provided by our scheme in [AB09].

2 System Architecture

A typical credit card mechanism consists of cardholders (consumers), merchants (sellers), Card Issuing Banks, Acquiring Banks and Credit Card Associations.

When eligible to receive a credit card, a consumer applies to a *Card Issuing Bank* she maintains an account with. The *Card Issuing Bank* bills the *cardholders* for payment and bears the risk of fraudulent use of the card. On the other hand, *Merchants*, who are eligible to receive credit card payments, are in agreement with an *Acquiring Bank* authorized to receive payments on their behalf. Banks are organized in *Credit Card Associations* (such as Visa® or Master Card®) that set the transaction rules between *Card Issuing* and *Acquiring Banks*.

For convenience, in the following sections, we will refer to a merchant as 'he', to a client as 'she' and to any type of Bank as 'it'. In addition, we will use the following acronyms: CIB for Card Issuing Bank, AB for Acquiring Bank, ACCA for our Anonymous Credit Card Association and ACC for Anonymous Credit Card.

As we aim to create a realizable system, we assume that our adversary has all the powers and motives real Banks/merchants/cardholders or groups of them would have. In addition, we assume that all parties have as main objective to increase their profit and would not act against it. More specifically:
a. All of banks are "honest but curious": they are trusted to do their functional operations correctly, but they may collude with each other or with merchants and combine the information they possess to track their customers' activities.
b. Merchants are mostly interested in receiving their payment. However, they may try to "deceive" a cardholder into making her pay more. For advertising purposes, merchants may be motivated — if cost effective — to collaborate with banks to profile their customers. In offline transactions the merchant knows the customer's face. However, any attempt to identify a customer manually (i.e. by comparing pictures online) is not cost effective and is thus highly unlikely.
c. Cardholders may try to "cheat", i.e. not to pay a merchant, to forge an ACC, or perhaps to frame another customer by accusing her of having cheated.

3 Requirements

Privacy and the rest of our system requirements will be presented in this section. For simplicity (and since we assumed collaboration between banks), we will refer to all of them as a united organization, a general Bank.

Privacy. Given a simple (online) cardholder-merchant transaction, no unauthorized third party — including the bank — should be able to gain any information regarding that particular transaction or link it to a particular cardholder even with merchant's collaboration (We call this *Customer Anonymity w.r.t bank and the merchant*). In addition, linking different ACC-based transactions as having been done by the same cardholder should be impossible (*Transaction Unlinkability*). However, we require that the privacy provided in our system is *conditional*: guaranteed for honest cardholders, but immediately revoked for dishonest ones.

As mentioned before, one of our fundamental requirements is the system's **Deployability**, i.e. our protocols should be usable with the current credit card systems' architecture as described in the previous section. **Credit Card Unforgeability** and **non-Transferability** are also required; our cards should not be forgeable or usable by any third party. It should be possible for cardholders to track their transactions (**Expense Report Service**) and provide an undeniable proof of any mischarge (**Error Correction Service**) without endangering their privacy. Privacy-preserving **Loss Recovery** of the card and **Special** payment rate **offers** should be supported.

4 Anonymous Credit Card System

A credit mechanism can be viewed as a long term loan. The cardholder is credited the amount she borrows to transact, while credit limit $\mathsf{L}_{\mathsf{credit}}$ is the highest loan balance that is authorized. To avoid charges for a more than she has spent, the customer is required — at the end of each month — to provide undeniable proof of the amount of money she has spent within that month. In this section we will provide a brief presentation (see [AB09] for more details) of the most important services of our system: ACC payment, Merchant payment, Loss recovery, and Expense report service.

Payments are realized through the use of two types of ecash -wallets presented at [CHL05] withdrawn at the *ACC Issue* procedure: the payment wallet W_p, which — if spent more than its value — reveals the cardholder's identity and the identity wallet W_{id}, which — if overspent — reveals the entire transaction activity of the double-spender. The two wallets have an equal number of

electronic coins (ecoins), which is proportional to the cardholder's credit limit $\mathsf{L}_{\mathsf{credit}}$. To enforce different privacy levels, various combinations of these wallets' spendings are used in the *ACC-payment procedure*, where the product value is spent from both wallets; in *ACC-loss recovery*, where only W_p is used; and in *ACC-monthly payment calculation*, where only W_{id} is used. To get paid, merchants simply deposit the ecash they receive, while blind signature schemes [JLO97,LR98,O06] are used for the different types of market offers.

In what follows we will use $[\mathsf{B}]\mathsf{Sig}_{\mathsf{C}}(\mathsf{Msg})$ ($[\mathsf{B}]\mathsf{Sig}^{\mathsf{H}}_{\mathsf{C}}(\mathsf{Msg})$) to denote the [blind] signature of C on Msg ($\mathsf{H}(\mathsf{Msg})$) and $\{\mathsf{Msg}\}_K$ to denote encryption of Msg under key K. For efficiency, every asymmetric encryption is inducted to a symmetric one: $\{\mathsf{Msg}\}_{PK}$ denotes $\{K\}_{PK}||\{\mathsf{Msg}\}_K$ for a random K.

Setup. CIBs maintain a large database consisting of their customers' account information: D_{debit}, for customers' debit accounts, D_{credit} for credit accounts, D_{anon}, for temporary anonymous accounts used only in online ACC transactions, and D_{hist} which is used as a log of D_{credit} and D_{anon}. ABs, which may or may not be CIBs, are linked to merchants' debit accounts.

In addition to the signature key pair $(pk^s_{\mathsf{B}}, sk^s_{\mathsf{B}})$ which identifies it, each CIB carries out the appropriate setup process to support the two compact ecash schemes in [CHL05]. The ACCA chooses and publishes (online) transaction-related hashes (H_{ot}) H_t and H_r.

Merchants and Cardholders are identified by the signature keys they use when opening an account with a bank B. Each party collaborates with B to issue a digital signature key-pair (pk^s_x, sk^s_x), where $x = \mathsf{M}$ or C. Each merchant M also obtains a validity certificate $\mathsf{Cred}_{\mathsf{M}} = \mathsf{Sig}_{\mathsf{B}}(pk^s_{\mathsf{M}})$. Customer's C signature key-pair, $(pk^s_{\mathsf{C}}, sk^s_{\mathsf{C}})$, is strongly connected with her transaction activity; a part of it is revealed when C misbehaves.[1]

ACC Issue. (Cardholder C–CIB CIB interaction) A CIB CIB and its customer C collaborate so that the latter can withdraw from the $\mathsf{L}_{\mathsf{credit}}$-size payment W_p and identity W_{id} wallets. It is a typical withdrawal of the two ecash schemes in [CHL05], for which C provides her sk^s_{C}-related password, $pass_{pin}$. Public information regarding the banks participating in ACCA (params) is also stored in ACC.

C also chooses a set of passwords: a backup $pass_e$ password, from which her backup encryption key pair $(pk^e_{\mathsf{C}}, sk^e_{\mathsf{C}})$ is derived, and $pass^t_e$, $pass^w_e$, $pass^c_e$ — which correspond to three encryption key-pairs $(pk^{e_t}_{\mathsf{C}}, sk^{e_t}_{\mathsf{C}})$, $(pk^{e_w}_{\mathsf{C}}, sk^{e_w}_{\mathsf{C}})$, and $(pk^{e_c}_{\mathsf{C}}, sk^{e_c}_{\mathsf{C}})$ that serve for encryption of transaction, wallet and coupon part

[1] In reality, there are two key-pairs issued by C; each is indicative of C and corresponds to the two ecash schemes in [CHL05]; for simplicity, we will refer to both as $(pk^s_{\mathsf{C}}, sk^s_{\mathsf{C}})$.

of the card, as we will describe later on. C also agrees on two hashes, H_K and H_{CB}, with B.

Offline Payment. (ACC–merchant machine interaction) Merchant M provides $\mathsf{Cred_M}$ to the cardholder C, who checks its validity using params. M provides C with $(\mathsf{Cred_M}, T_{det}, \mathsf{Sig}_{\mathsf{M}}^{H_t}\{T_{det}\})$, where T_{det} is the transaction information, including *price* and *date*. C enters her $pass_e^w$ to have her W_p and W_{id} wallets decrypted, verifies the product information and inserts her $pass_{pin}$ to spend *price* value from both wallets. Let W'_p and W'_{id} be the remaining wallets. C is immediately provided a printed transaction record. A merchant-signed receipt, $\mathsf{Rec_T} = \mathsf{Sig}_{\mathsf{M}}^{H_r}(\mathsf{Cred_M}, T_{det} - fin)$, and T_{det} are encrypted with $pass_e^t$ $(pk_{\mathsf{C}}^{e_t})$ into $E_{T_{det}}$ and stored in the ACC. C also uses her $pass_e^w$ $(pk_{\mathsf{C}}^{e_w})$ to encrypt W'_p and W'_{id} into $E_{W_{p,id}}$.

To receive his payment, M deposits to his AB (AB) the ecoins he has received from his customers. In particular, AB contacts each customer's CIB to validate each pair of payment-identity ecoins deposited by M. If everything is fine, both banks make the required transfers to M's account. On the other hand, if a cardholder C tries to use her ACC to spend more than $\mathsf{L_{credit}}$ value, i.e. if a double-spending occurs, the owner of the card is identified through the ecash anonymity revocability properties. If the latter is the case, all the ecoins the dishonest C withdrew are blacklisted.

Online Payment is performed in two stages:
Anonymous Account Setup.(ACC–ATM interaction) Cardholder C spends to her CIB (CIB) M_{ot} value from her W_p, W_{id} wallets, where M_{ot} is the amount to be spent online. To refer to M_{ot}, C chooses m, R_{ot}, hashes H_{ot} and H_α and a pseudonym key-pair $(pk_{\mathsf{C}}^P, sk_{\mathsf{C}}^P)$. C computes $A_{\mathsf{C}}^m = H_{ot}^{(m)}(R_{ot})$ and sends to CIB the message:

$$\{A_{\mathsf{C}}^m, m, H_{ot}, H_\alpha, pk_{\mathsf{C}}^P\}.$$

CIB updates D_{anon} with

$$\alpha_{\mathsf{C}}(m) = \{A_{\mathsf{C}}^m, H_{ot}, M_{ot}, m, H_\alpha, pk_{\mathsf{C}}^P\}$$

and sends a confirmation to C $\mathsf{Rec}_{\alpha_{\mathsf{C}}(m)} = \mathsf{Sig}_{\mathsf{CIB}_{ot}}(H^r(\alpha_{\mathsf{C}}(m)), date)$. A_{C}^m will be the initial number of the anonymous account created and m is the upper bound of the number of transactions C can participate in using the online account she created.
Transaction Payment. (Cardholder C–gateway G online interaction) The cardholder C provides the merchant's (M) website or the gateway G behind it with:

$$\mathsf{Info_{CIB}} = \{\{\mathsf{Cred_M}, T_{det}, A_{\mathsf{C}}^{m-1}\}_{K_\alpha}, A_{\mathsf{C}}^m\}_{\{pk_{\mathsf{CIB}}^e}$$

where $\mathsf{Cred_M}$ is M's credential, T_{det} the transaction details and $K_\alpha = H_\alpha(A^m_\mathsf{C}))$ is a key derived from C-chosen H_α and A^m_C. Both A^{m-1}_C and K_α are used for authentication purposes; the owner of A^m_C account is the only one who knows H_{ot}, H_α and A^m_C's pre-image. G sends $\mathsf{Info_{CIB}}$, $\mathsf{Cred_M}$ and T_{det} to C's CIB (CIB) for it to check the A^m_C's validity and balance. CIB sends G either a payment check $\mathsf{Paym_{CIB\rightarrow AB}}$ for merchant's AB (AB) or a signed rejection message $\mathsf{Rej_{CIB}}$ in case of error. All messages are signed and contain T_{det} and timestamps to avoid confusion and replay attacks. G forwards $\mathsf{Paym_{CIB\rightarrow AB}}$ to AB and acknowledges CIB with

$$\mathsf{Rec_T} = \mathsf{Sig}^{H_r}_\mathsf{G}(\mathsf{Cred_M}, T_{det} - fin)$$

. CIB updates D_hist with $\mathsf{Rec_T}$ and substitutes $\alpha_\mathsf{C}(m)$ $D_\mathsf{anon}$entry with $\alpha_\mathsf{C}(m-1)$, where the M_{ot} is reduced by *price* or not depending on whether CIB accepted or rejected the request. To close the entry in D_anon, C, in an ACC-ATM interaction, demonstrates knowledge of $\mathsf{Rec}_{\alpha_\mathsf{C}(m)}$ and her ACC context is updated accordingly.

ACC BackUp - Loss Recovery. (Cardholder C–CIB CIB in-person interaction) *ACC BackUp.* Cardholder C generates a random number N_b and sends to her CIB CIB

$$\{N_b\}_{pk^e_\mathsf{C}} \text{——} \{ACCcontent \text{——} date - time\}_K$$

where $ACContent$ is the content of the ACC, $date-time$ is the backup timestamp and $K = H_K(N_b, pass_{pin})$ is a symmetric encryption key, which only C may derive given N_b. $BackUp$ is hashed and signed by both parties for integrity purposes into $BackUp_x = Sig^{H_{CB}}_x(BackUp), x = \{\mathsf{C}, \mathsf{B}\}$. CIB updates D_hist. *Loss Recovery.* Cardholder C is provided by her CIB CIB with the most recent BackUp of her ACC, $BackUp$. C verifies that $BackUp$ matches the most recent $BackUp_B$ of her and spends to the latter the $BackUp$'s remaining payment wallet (W'_p). CIB credits C's entry in D_credit for the amount spent till $BackUp$ was taken ($\mathsf{L_{credit}}$ - $|W'_p|$, where $|W'_p|$ are the remaining value (ecoins)of W'_p. When merchants' deposit ends, CIB updates C's credit entry with any double-spent payment-ecoin indicating C's pk_C. In this way, we cover the case where $BackUp$ is not up-to-date with the most recent transactions of C without sk_C being revoked. Based on current D_credit Centry, CIB and C collaborate to issue an ACC with the new or different credit limit.

Monthly Payment Calculation. (Cardholder C–CIB in-person interaction) Cardholder C proves to CIB the amount of money she has spent throughout the past month month. To calculate C's monthly payment, C's CIB, CIB, applies the formula used in current Credit Card Systems on C's overall credits.

After decrypting (via $pass_e^w$) the remaining of her W_{id} wallet (W'_{id}), C interacts with CIB to spend it entirely. The amount of ecoins spent by C through the past month is $\mathsf{L_{credit}}$ - $|W_i d'|$ and CIBcan now estimate the monthly payment for C. If C is still eligible for an ACC, she interacts with CIB to issue a new W_{id} and additional W_p according to C's new credit limit. Any attempt on C's part to lie for the remaining W_{id} wallet, e.g., by presenting a former version of her ACC, would reveal sk_{C}^s since a part of W_{id} will be spent twice.

Expense Report. For offline transactions or for online transactions of deactivated anonymous accounts, C decrypts $E_{T^i_{det}}$ parts of her ACC to obtain the detailed chain of her transactions. For online transactions referring to active anonymous accounts, C in an ACC-ATM interaction with CIB, sends through her sends a $\mathsf{Info_{CIB}}$ message with expense report request message instead of T_{det}. CIB sends back the corresponding report and updates D_{anon} accordingly. See [AB09] for more details.

Error Correction.(Cardholder C–ACCA/Merchant in-person interaction) If an error has occurred, e.g., a mischarge by M, C contacts the ACCA and provides it with $\mathsf{Rec_T}$. ACCA contacts M, who may accept ($\mathsf{Ref_M}$) or reject ($\mathsf{Rej_M}$) the refund-request (see [AB09]). If M accepts, the ACCA sends $\mathsf{Ref_M}$ to M's AB, AB, to verify M's account balance. AB provides ACCA the actual payment, which is forwarded to C's CIB CIB. C deposits to CIB an ACCA-issued digital check, $\mathsf{RefCoup_{ACCA \to C}}$, to receive the payments in the form of wallets. In case of purchase cancellation, if M accepts the return of the product, it provides C with $\mathsf{Ref_M}$, which C deposits to her CIB.

ACC Promotion Offers These offers involve discounts or better credit card interest rates, when a carholder makes many purchases from particular merchants. This option is supported by our system through the use of blind coupons only offer-eligible merchants may issue. However, as it does not constitute a core attribute of a credit card system and because of space limitations, we will not elaborate on it here. See [AB09] for details.

5 Other System Considerations

We will now outline particular system issues. See [AB09] for a full discussion.

Cardholder Anonymity - Transaction Unlinkability. Both of them are satisfied through ecash anonymity and unlinkability properties [CHL05]. As every payment procedure (including the anonymous account setup) consists of two

typical ecash spending procedures from the W_p and W_{id} wallets, they thus cannot be linked to the cardholder C who used the ACC or to any other transaction from the same wallets (ACC). However, the anonymity provided is conditional: if C tries to spend more ecoins than her $\mathsf{L}_{\mathsf{credit}}$, i.e., the initial amount of ecoins in each wallet, or lie at the monthly payment calculation procedure for the amount she has spent, a part of W_{id} will inevitably be double-spent, and — through anonymity revocability and traceability property of the W_{id} ecash scheme [CHL05] — sk^s_{C} will be revealed; all the ecoins withdrawn by C will then be traced.

There are two cases in which we accept a small breach in a cardholder's anonymity or transaction unlinkability: (a) in *Loss Recovery* and (b) in *Online Payment*. In the Loss Recovery process — an unusual situation — when the most recent $BackUp$ is not up-to-date, a cardholder C inevitably doublespends a part of her W_p wallet: to the merchants she interacted and to her CIB, CIB. pk^s_{C} is then revealed and CIB knows whom C interacted with. However, this anonymity breach becomes less important since we require that backups are taken regularly. In the *Online Payment* case, CIB can obviously trace what type of transactions a particular anonymous account is involved in through D_{hist}. However, thanks to the unlinkability property of the ecash spent at the anonymous account setup phase, linking that profile to a particular identity is impossible. In any case, the cardholder may open as many anonymous accounts she wishes, in order to avoid transaction linkability.

Security of Online Transactions. Customer C authentication is achieved via (a) the $pass_{pin}$ C enters to setup the A^m_{C} anonymous account and through (b) demonstration of knowledge of H_{ot}, H_α and A^m_{C}'s pre-image w.r.t. H_{ot}. On the other hand, the signed endorsement $Rec_{A^m_{\mathsf{C}}}$ provided by C's CIB, CIB, at the $\alpha_{\mathsf{C}}(m)$ setup phase prevents CIB from cheating. As T_{det} and $\mathsf{Cred}_{\mathsf{M}}$ are part of $\mathsf{Info}_{\mathsf{CIB}}$, i.e., encrypted with K_α, a key only CIB and C may derive, G cannot lie about the price of C's intended purchase (*price*) or M. In addition, as timestamps are included in every message and account numbers change in every authorized request, replay attacks or offline account guessing attacks cannot succeed.

On the other hand, C cannot use the same account for purchases of value more than M_{ot}: if she tries to spend the same part of her wallets in offline purchases, her identity will be revoked while if the account balance is less than *price*, she will receive a CIB signed rejection message. In addition to the measures mentioned before, we assume that there is an upper bound for M_{ot} and that the latter is spent within a particular time interval to reduce the amount of transaction-wise information bound to each anonymous account.

Authorized Anonymity Revocation. This is the case where a cardholder C is a suspect of a offense and a judge requests a detailed description of that C's ACC related transactions. In our system, this can be achieved only with C's consent. *a.* $\mathsf{C}$is asked to provide sk^s_{C} for all her transactions to be revealed, which we want to avoid. *b.* $\mathsf{C}$is asked to enter her $pass^t_e$ to decrypt the transaction related part of her ACC and "spend" the rest of her W_p to CIB. Transaction details of each transaction are signed by a merchant or C's CIB (CIB) — in the case of $\mathsf{Anonymous\ Account\ Setup}$ — and, thus, cannot be forged. To check for any deceptive deletion of a transaction on cardholder's side, CIB may use D_{hist} to check whether the overall amount spent matches the aggregated amount in the backed-up transaction details.

ACC Unforgeability is satisfied through the Correctness and Unforgeability properties of the underlying ecash schemes. **ACC non-Transferability** is also satisfied since sk^s_{C} is required for the card to be used in both offline and online purchases.

Bank Dishonesty. $BackUp_{\mathsf{B}}$ is used to avoid any attempt of a CIB to trick a cardholder into tracing more of the latter's transactions: Assuming the CIB provided a less recent backup, then a bigger part of W_p would be double-spent and more merchants would be directly linked to the cardholder. $BackUp_{\mathsf{B}}$ will act as an undeniable proof of the date and integrity of the backup kept.

ACC Organization. ACCs' content is organized as $\{E_{T^1}, \ldots, E_{T^\ell}, padding, E_{W'_{p,id}}\}$, where E_{T^1} is the encryption of the i-th transaction performed by an ACC and ℓ is the number of transactions the performed through that particular ACC. We use $padding$ to avoid any information leakage regarding ℓ. This modular form of encryption is necessary for each of the procedures mentioned before to be able to be executed individually.

Computing power. Credit card customers in our system often lack in computing sophistication: not all of them have or know how to install software able to encrypt or decrypt text or verify the hashes used in our system. A solution on this problem would be for the CIBs to provide their customers with special machines dealing with card encryption/decryption issues. The extra cost of these devices may be viewed by the cardholder as an extra price for her privacy.

6 Conclusion

In this paper, we addressed e-commerce Context Privacy. In particular, we presented a deployable credit card system which guarantees cardholder anonymity and transaction unlinkability, even towards to Credit Card Associations or Card Issuing Banks. At the same time, we have preserved many of the essential benefits of credit cards. In special circumstances the transactions of a party may be revealed but only with that party's consent. Undeniably, there are still issues to be dealt, such as password loss recovery and operational transparency with respect to cardholders. However, we do believe that this paper is a good start for privacy in current credit card systems.

7 Acknowledgments

The authors would like to thank Moti Yung and the anonymous referees for their valuable comments and suggestions and Google Inc. for subsidizing this work.

References

[AB09] E. Androulaki and S. Bellovin. Anonymous credit cards. Technical Report cucs-010-09, Columbia University, New York, USA, 2009.

[AJSW99] N. Asokan, P. Janson, M. Steiner, and M. Waidner. State of the art in electronic payment systems. *IEEE Computer*, 30:28–35, 1999.

[B95] S. Brands. Electronic cash on the internet. In *Proceedings of the Symposium on the Network and Distributed System Security*, 1995.

[BBG+00] M. Bellare, M. Bellare, J. Garay, R. Hauser, H. Krawczyk, A. Herzberg, G. Tsudik, E. van Herreweghen, H. Krawczyk, M. Steiner, G. Tsudik, E. V. Herreweghen, and M. Waidner. Design, implementation and deployment of the ikp secure electronic payment system. *IEEE Journal on Selected Areas in Communications*, 18:611–627, 2000.

[CHL05] J. Camenisch, S. Hohenberger, and A. Lysyanskaya. Compact e-cash. In *Advances in Cryptology - EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 302–321. Springer-Verlag, 2005.

[CL02] J. Camenisch and A. Lysyanskaya. A signature scheme with efficient protocols. In *International Conference on Security in Communication Networks – SCN*, volume 2576 of *Lecture Notes in Computer Science*, pages 268–289. Springer Verlag, 2002.

[DCN90] A. F. D. Chaum and M. Naor. Untraceable Electronic Cash. 1990.

[JLO97] A. Juels, M. Luby, and R. Ostrovsky. Security of blind digital signatures (extended abstract). In *Advances in Cryptology - CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science*, pages 150–164. Springer-Verlag, 1997.

[K99] H. Krawczyk. Blinding of credit card numbers in the set protocol. In *FC '99: Proceedings of the Third International Conference on Financial Cryptography*, pages 17–28, London, UK, 1999. Springer-Verlag.

[LPM94] S. H. Low, S. Paul, and N. F. Maxemchuk. Anonymous credit cards. In *CCS '94: Proceedings of the 2nd ACM Conference on Computer and communications security*, pages 108–117, New York, NY, USA, 1994. ACM.

[LR98] A. Lysyanskaya and Z. Ramzan. Group blind digital signatures: A scalable solution to electronic cash. In *In Financial Cryptography (FC)*, pages 184–197. Springer-Verlag, 1998.

[O06] T. Okamoto. Efficient blind and partially blind signatures without random oracles. In *TCC*, pages 80–99, 2006.